Intrusion detection based on K-means clustering and Naïve Bayes classification

ABSTRACT

Intrusion Detection System (IDS) plays an effective way to achieve higher security in detecting malicious activities for a couple of years. Anomaly detection is one of intrusion detection system. Current anomaly detection is often associated with high false alarm with moderate accuracy and detection rates when it's unable to detect all types of attacks correctly. To overcome this problem, we propose an hybrid learning approach through combination of K-Means clustering and Naïve Bayes classification. The proposed approach will be cluster all data into the corresponding group before applying a classifier for classification purpose. An experiment is carried out to evaluate the performance of the proposed approach using KDD Cup'99 dataset. Result show that the proposed approach performed better in term of accuracy, detection rate with reasonable false alarm rate.

Keyword: Intrusion detection system; Anomaly detection; Hybrid learning; Clustering; Classification